

Приблизний перелік індивідуальних завдань для проходження науково-дослідної практики студентів 2 -го курсу

1. Загрози безпеці інформації.
2. Сучасний стан законодавчого та нормативно-правового забезпечення захисту інформації.
3. Основні канали витоку мовної інформації та інформації, що передається у телекомунікаційних мережах та системах зв'язку, методи та засоби її захисту.
4. Закриття мовних сигналів у телефонних каналах, цифрові системи закриття мовних сигналів в каналах зв'язку.
5. Міжнародні та національні стандарти в галузі взаємодії відкритих систем і систем передачі інформації.
6. Загрози інформації у комп'ютерних системах.
7. Методологія захисту комп'ютерних систем.
8. Політика безпеки комп'ютерних систем, моделі та механізми захисту.
9. Критерії та оцінки захищеності комп'ютерних систем, методика оцінювання захищеності комп'ютерних систем.
10. Криптографічні засоби захисту інформації.
11. Шифри з відкритими ключами, розподіл ключів, криптографічні протоколи.
12. Автентифікація інформації, цифровий підпис.
Матеріали, що отримав студент під час виконання індивідуального завдання, можуть в подальшому бути використані для виконання кваліфікаційної роботи, для підготовки доповіді, статті або для інших цілей за погодженням з кафедрою і базою практики.
13. Методи підвищення ефективності алгоритмів ймовірнісної факторизації для різних моделей обчислень.
14. Дослідження та оптимізація швидкої платформи-незалежної реалізації алгоритму ЕЦП, встановленого ДСТУ 4145-2002
15. Модель застосування гомоморфної криптографії для пошуку даних.
16. Методи побудови анонімних мереж з використанням багаторівневої криптографії.
17. Тести оцінки лінійної складності випадкових послідовностей.